The Development of NASA's Fault Management Handbook

Neil Dennehy, NASA Goddard Space Flight Center, Greenbelt, MD, USA

Lorraine Fesq, Jet Propulsion Laboratory, California Institute of Technology, Pasadena, CA, USA

Abstract

Fault management (FM) is a maturing discipline; currently there is no unifying description or set of guidelines for this field. Disciplines related to FM such as Reliability and Hazard Analysis do have formal methodology documents, and in some cases, NASA Procedural Requirements to guide development of the work products. However, none fully addresses the needs of FM. FM is a key factor to increase safety, reliability, availability, and performance in systems, and requires the rigor of other safety-critical processes in order for significant improvements to be made. Without this rigor, improvements to safety and reliability will be limited.

A number of approaches to FM have been tried, and while many of these have been locally successful, they are inconsistent with each other and often deal with FM issues in a fragmented way. Currently it is difficult to assess the appropriateness of the architecture selected, the quality of the processes used and the development of interfaces, which can lead to designs that are complex and/or difficult to verify and validate. All of these approaches have difficulty addressing questions of completeness and effectiveness.

NASA is developing a FM Handbook to establish guidelines and to provide recommendations for defining, developing, analyzing, evaluating, testing, and operating FM systems. It establishes a process for developing FM throughout the lifecycle of a mission and provides a basis for moving the field toward a formal and consistent FM methodology to be applied on future programs. This paper describes the motivation for, the development of, and the future plans for the NASA FM Handbook.

Background

In 2008, the NASA Science Mission Directorate (SMD), Planetary Science Division, commissioned the first NASA FM Workshop[1] in response to a number of technical and programmatic issues surrounding FM experiences on numerous missions. The workshop was held in April 2008 in New Orleans, Louisiana. Although the workshop was to address a pattern of problems occurring across several planetary missions, the participants concluded that the challenges of adequate FM are present to a degree in all space missions. A primary recommendation from the workshop was the development of an FM Handbook that would benefit not only planetary missions but also all NASA missions. The NASA Chief Engineer and the NASA Constellation Program Chief Architect endorsed the development of an FM Handbook.

[1] Fesq, Lorraine (ed). *NASA White Paper Report: Spacecraft Fault Management Workshop Results for the Science Mission Directorate*, Pasadena, CA: NASA Jet Propulsion Laboratory. 2009.

In 2010, the NASA Science Mission Directorate's Discovery and New Frontiers Program Office and the Office of the Chief Engineer's NASA Engineering & Safety Center (NESC) co-sponsored the development of the Handbook as an initial step to coalesce the FM field. As a result of this sponsorship, the initial focus addresses FM required for science missions. It is recognized that FM is relevant to all NASA missions, and that ultimately the Handbook should address the needs of the Agency. In preparation for this broadened scope, the authors have strived to develop an outline that identifies FM-related needs and goals for all Directorates, with the intent that the content for the Aeronautics Research Mission Directorate and the Human Exploration and Operations Mission Directorate will be completed in a future revision of the Handbook.

The Scope of Fault Management

FM is an engineering activity; it is the part of systems engineering (SE) that addresses the off-nominal behavior of a system, as well as a subsystem that has to be designed, developed, integrated, tested and operated. FM encompasses functions that enable an operational system to prevent, detect, isolate, diagnose, and respond to anomalous and failed conditions interfering with intended operations. From a methodological perspective, FM includes processes to analyze, specify, design, verify, and validate these functions. From a technological perspective, FM includes the hardware and control elements, often embodied in software and procedures, of an operational system by which the management of faults and anomalous situations is realized. It includes a situation awareness capability such as caution/warning functions to notify operators and crew of anomalous conditions, hazards, and automated responses. The primary goal of FM is the preservation of system assets, including crew, and of intended system functionality (via design or active control) in the presence of failures.

FM demands a system-level perspective, as it is not solely a localized concern. A system's design is not complete until potential failures are addressed, and comprehensive FM relies on the cooperative design and operation of separately deployed system elements (e.g., in the space systems domain: flight, ground, and operations deployments) to achieve overall reliability, availability, and safety objectives. Like all other system elements, FM is constrained by programmatic and operational resources. Thus, FM practitioners are challenged to identify, evaluate, and balance risks to these objectives against the cost of designing, developing, validating, deploying, and operating additional FM functionality.

FM as a discipline is still in the formative stage,[2] as reflected by the different approaches used in many organizations, and by the ongoing activities to gain community consensus on the nomenclature. In fact, the term "fault management" is in itself something of a misnomer—the discipline of FM is concerned with failures in general and not just faults ,which are failure causes rooted within the system,. However, present use of the term "fault management" is synergistic with usage in the field of network management, where

[2] Yet as a practice, significant heritage exists for FM designs, analyses, and verification and validation processes.

the International Organization for Standardization[3] (ISO) defines FM as "the set of functions that detect, isolate, and correct malfunctions…." Likewise, the above-stated goal of FM (i.e., preservation of system assets and intended system functionality in the presence of failures) is consistent with the ISO-stated goal of having "a dependable/reliable system in the context of faults."

FM is crucial to the successful design, development, and operation of all critical systems (e.g., communications networks, transportation systems, and power generation/distribution grids). However, the architectures, processes, and technologies driving FM designs are sensitive to the needs and nature of the development organization, the risk posture, the type of system under development, and the targeted operating domain. Within NASA, FM is crucial to the development of crewed and un-crewed robotic systems in service of science,[4] in the development of flight controls and maintenance of aircraft, and in the procurement, contractual oversight, and acceptance of commercial launch vehicles and orbital transportation services.

The Development of the FM Handbook

[Discuss putting together the team, laying out an outline that met the needs of the agency, and focusing on planetary and earth orbiters for first version. Describe how the team worked, telecons, WebEx, document sites, face-to-face kick-off, etc. Division of Sections – lead author(s), designated reviewers. An overview/slide presentation of each Section was presented to the team for comment prior to writing to allow input from all team members. External Review Team. Discuss the FM Community of Practice.

The Contents of the FM Handbook

The following bullets capture the outline of the FM Handbook, and provides insights into the contents of key sections.

- Foreward – Explains why NASA needs a FM Handbook and describes what this Handbook provides;
- Scope – Describes what is meant by FM, its relevance across the agency, and intended users of the Handbook;
- Definitions – An attempt to unify the terminology used in this field;
- Concepts and Guiding Principles -- guiding principles grounding the field, describing FM functions, FM as part of SE, FM goals: asset and function preservation;
- Organization, Roles and Responsibilities – Suggested project organizational structure to support FM, interfaces and tasks;
- Process – Follows the NASA SE process but focuses on developing FM products including concept design, requirements, architecture, analysis, V&V, operations and maintenance;

[3] International Organization for Standardization. *Information Technology — Multimedia Middleware — Part 6: Fault management, ISO/IEC 23004-6:2008.* Geneva, 2008.

[4] NASA's robotic systems include terrestrial and non-terrestrial systems including aircraft, dirigibles, submersibles, rovers, rockets, satellites, space stations, space probes, telescopes, and other *in situ* platforms.

- Requirements Development – Defines FM requirements categories, identifies driving requirements and flowdown;
- Design and Architecture – Explains the impacts of mission risk posture, goals and characteristics on FM priorities, provides insights into FM architectures, design features and approaches; highlights mission-specific considerations
- Assessment and Analysis – will be supplied in later releases
- Verification and Validation – Identifies FM V&V planning and preparation, how to perform FM V&V and to analyze results, selection and prioritization of FM test scenarios, ensuring sufficient capabilities in simulators, testbeds and ground support equipment to test for responses to anomalies and faults.

Conclusions and Future Plans

The FM Handbook is a first step taken by NASA to coalesce the discipline. It offers guidelines and recommendations for defining, developing, analyzing, evaluating, testing, and operating the FM element of flight systems. The Handbook establishes a process for developing FM throughout the lifecycle of a mission and provides a basis for moving the field toward a formal and consistent FM methodology to be applied on future programs. The insights and concepts captured in the Handbook provide a basis for moving the field toward a formal and consistent FM methodology to be applied on future programs.

The Handbook in its current state is, admittedly, incomplete in two respects. First, a number of Sections were identified in the outline but have not yet been written due to lack of resources. Second, the Handbook captures concepts that are derived from robotic orbiters and deep space missions, which is only a part of NASA's purview. FM is recognized as being an essential element of all NASA missions, and as such, the Handbook must also respond to the needs of human spaceflight, ground systems, mission systems and aeronautics, and must integrate seamlessly with functions performed by the NASA Office Safety and Mission Assurance. Activities currently are underway to bridge the gaps that exist between these communities, including activities to gain consensus on FM nomenclature.

Acknowledgements

The authors of this paper acknowledge the following persons who worked as a team to co-author the FM Handbook: Timothy Barth, NASA Kennedy Space Center and NESC Systems Engineering Office; Micah Clark, Jet Propulsion Laboratory, California Institute of Technology; John Day, InSpace Systems (JPL Affiliate); Kristen Fretz, Johns Hopkins University, Applied Physics Laboratory; Kenneth Friberg, Friberg Autonomy (JPL Affiliate); Stephen Johnson, NASA Marshall Space Flight Center (MSFC) and University of Colorado, Colorado Springs; Philip Hattis, Draper Laboratory; David McComas, NASA Goddard Space Flight Center; Marilyn Newhouse, Computer Science Corporation (MSFC Affiliate); Kevin Melcher, NASA Glenn Research Center; Eric Rice, Jet Propulsion Laboratory, California Institute of Technology; John West, Draper Laboratory; and Jeffrey Zinchuk, Draper Laboratory.

The following people contributed to the FM Handbook as reviewers: Michael Battaglia, NASA Headquarters, Office of the Chief Technologist; Brad Burt, Jet Propulsion

Laboratory, California Institute of Technology; Tim Crumbley, NASA Marshall Space Flight Center, NESC Software Engineering Representative; Fernando Figueroa, NASA Stennis Space Center; Steve Hogan, The Aerospace Corporation; Brian Kantsiper, Johns Hopkins University, Applied Physics Laboratory; Richard Larson, NASA Dryden Flight Research Center; Ken Lebsock, Orbital Sciences Corporation (GSFC Affiliate); and Steve Scott, NASA Goddard Space Flight Center

Part of the research was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration.